Remarks/Arguments

Reconsideration of this Application is requested.

Stefik discloses the following in his abstract:

"A system for controlling use and distribution of composite digital works. A digital work is comprised of a description part and a content part. The description part contains control information for the composite digital work. The content part stores the actual digital data comprising the composite digital work. The description part is logically organized in an acyclic structure, e.g. a tree structure. For a composite digital work each node of the acyclic structure represents an individual digital work or some distribution interest in the composite digital work. A node in the acyclic structure is comprised of an identifier of the individual work, usage rights for the individual digital work and a pointer to the digital work. Composite digital works are stored in repositories. A repository has two primary operating modes, a server mode and a requester mode. When operating in a server mode, the repository is responding to requests to access digital works. When operating in requester mode, the repository is requesting access to a digital work. A repository will process each request to access a composite digital work by examining the usage rights for each individual digital work found in the description part of the composite digital work."

Stefik discloses the following in lines 1-31 of column 4:

"A digital work is comprised of a description part and a content part. The description part contains control information for the composite digital work. The content part stores the actual digital data comprising the composite digital work. The description part is logically organized in an acyclic structure (e.g. a tree structure.) For a composite digital work each node of the acyclic structure represents an individual digital work or some distribution interest in the digital work. A node in the acyclic structure is comprised of an identifier of the individual work, usage rights for the individual digital work and a pointer to the digital work. In this representation, the description part may naturally be stored separately on a separate medium from the content part.

Composite digital works are stored in repositories. A repository is comprised of a storage means for storing a digital work and its attached usage rights, an external interface for receiving and transmitting data, a processor and a clock. A repository has two

primary operating modes, a server mode and a requester mode. When operating in a server mode, the repository is responding to requests to access digital works. When operating in requester mode, the repository is requesting access to a digital work. A repository will process each request to access a composite digital work by examining the usage rights for each individual digital work found in the description part. Access is granted if the composite digital work if access to each of the individual digital works can be granted. [sic] Alternatively, if access to all the individual digital works cannot be granted, partial access can be granted only to those individual digital works which grant access."

Stefik discloses the following in lines 34-48 of column 6:

"In any event, Repository **1** checks the usage rights associated with the digital work to determine if the access to the digital work may be granted, step **105**. The check of the usage rights essentially involves a determination of whether a right associated with the access request has been attached to the digital work and if all conditions associated with the right are satisfied. If the access is denied, repository **1** terminates the session with an error message, step **106**. If access is granted, repository **1** transmits the digital work to repository **2**, step **107**. Once the digital work has been transmitted to repository **2**, repository **1** and **2** each generate billing information for the access which is transmitted to a credit server, step **108**. Such double billing reporting is done to insure against attempts to circumvent the billing process."

No archival copy is made between Stefik's steps 107 and 108 of Fig. 1. If Stefik's repository 1 fails and Stefik's repository 2 fails, the user is unable to obtain an archival copy of the material the user previously purchased. Furthermore, there is a chance that a copy of the protected material will be in repository 1 or repository 2. However, the possibility exists that there would not be a copy of the protected material when the consumer wants an archival copy of material for which the consumer has previously paid.

Appln. No.: 09/704,864
Amdt. Dated November 17, 2004
Reply to Office Action dated October 12, 2004

The Examiner stated on page 3 of the October 12, 2004, Final Rejection the following: "Stefik fails to explicitly disclose the steps of determining whether or not there is a existing copy of the protected material, and storing an existing copy of the protected material (or digital work) <u>from a plurality of sources of the protected material</u> automatically of archival purposes at a site remote from the consumer at the time the material was first obtained by the consumer. Masuda discloses a back-up recovery copies to provide disaster recovery."

Masuda, et al. discloses the following in column 2, lines 61-67:

"Broadly, the present invention provides an integrated DBMS solution to recover a primary site database based upon maintenance of a shadow copy of the primary site's database at a remote site. Both the primary site DBMS and the remote site DBMS support write-ahead logging protocol in which log records are written to a log data set before database updates are entered into external storage.

The remote site is initialized as a mirror image of the primary site by transmitting all database data and recovery logs from the primary site to the remote site. After initialization, the primary site periodically starts and stops the remote site as a tracker system to keep the shadow copy up-to-date using database recovery logs and data shipped from the primary site. When started as a "tracker," the remote DBMS logs are initialized, system data is rebuilt, and transaction status is determined.

Whenever the tracker system is restarted, an end log point is specified that is used as the log scan ending point for all data recovery done during the current recovery cycle. This end log point is recorded in the shadow database after each data recovery and is used as the log scan starting point for the next recovery cycle when the tracker function is restarted with a new set of logs received from the primary site. In order to maintain the shadow database, if a LOG (NO) is encountered - if an image copy of a database data set is either reorganized or LOAD-replaced - the primary site must transmit a new image copy of the database data set from the time of the last tracker restart.

When a disaster occurs at the primary site, the remote site becomes the takeover site. When restarting the remote DBMS as a take-over

system, the primary site's logs are used to implement a normal three-phase system restart. The logs from the last system checkpoint are scanned to determine the transaction status at the time of the system failure, and to determine the earliest point in the log that the recovery function will need to process for a forward log recovery phase. The remote DBMS log initialization and transaction status is also determined by Forward Log Recovery (FLR) and Backward Log Recovery (BLR) phases are executed.

In essence, Masuda is creating a mere copy of the existing data. Then, Masuda utilizes a tracker at a remote site to maintain up-to-date recovery logs and data that is shipped from the primary site. Masuda is backing up data from a primary and exclusive site of data and only contemplates a primary and exclusive site for the data. Applicants' consumer's resources are not ordinarily burdened in obtaining back up data; whereas, Masuda burdens the primary system for all data which is analogous to Applicants' consumer.

Masuda discloses the following in line 57, column 4 to line 6, column 5:

"Each client system **102** creates original user data files, or client files, which are stored within the corresponding client system if the client system is provided with a storage system. Regardless, the client systems **102** transfer client files to the primary site **103**. Transferring client files to the primary site **103** inherently provides a backup mechanism within the server for original client files stored within the client system. The storage manager **104** directs the client file to a storage device, or storage volume, within a primary storage pool **110**. The primary storage pool stores a primary copy of the client files. The storage manager **104** maintains a log **105** within the server database **106** listing the files stored within the primary storage pool **110** and the cache **130** of the primary site **103**. Once the client file is stored within a primary storage pool **110**, the storage manager **104** updates the server database **106** and logs the updates in log **105** at the primary site **103**."

Masuda backs up everything arbitrarily, whereas in Applicants' claim 1, steps (b) and (d), Applicants only make a copy of the protected material when the bookshelf is

informed that the protected material was first obtained by the consumer. Thus, Applicants only make a copy if there is not a copy on the bookshelf.

Neither Stefik nor Masuda, taken separately or together, discloses or anticipates automatically making an archival copy of the protected material at a site remote from the consumer. The foregoing is claimed in steps c) and d) of claim 1, which read as follows:

> c) determining whether or not there is an existing copy of the protected material;
>
> d) storing an existing copy of the protected material from a plurality of sources of the protected material automatically for archival purposes at a site remote from the consumer at the time the material was first obtained by the consumer.

Steps c) and d) of claim 1 provide for the situation when the site that sold the digital rights protected content stops vending the material for any reason, and the digital rights protected material on the consumer's computer is lost or damage, i.e., theft of the consumer's computer, damage to the computer, or computer storage medium, computer crashes, etc., the consumer will be able to obtain an archival copy of the material. This is unlike other back up technology in that it happens automatically at a remote site at the time the material was first obtained by the consumer.

Furthermore, neither Stefik nor Masuda, taken separate or together, discloses step e) of claim 1, namely: e) creating a pointer for the consumer to point to the stored archival material.

Applicants' pointer does not point to the digital work. Appellants' pointer points to the stored archival material.

In view of the above, claims 1-19 are patentable. If the Examiner has any questions, would he please telephone the undersigned at the telephone number noted below.

Respectfully submitted,

Ronald Reichman
Reg. No. 26,796
Attorney of Record
Telephone (203) 924-3854

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000